Advisory Action Before the Filing of an Appeal Brief	**Application No.** 10/673,239	**Applicant(s)** MORIOKA ET AL.	
	Examiner Christopher C. Johns	**Art Unit** 3621	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 28 May 2008 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☐ The period for reply expires _____months from the mailing date of the final rejection.
   b) ☒ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☐ For purposes of appeal, the proposed amendment(s): a) ☐ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: _____.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☒ Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). 5/5/08
13. ☒ Other: Note attached PTO-892 form.

/ANDREW J. FISCHER/
Supervisory Patent Examiner, Art Unit 3621

Christopher C Johns
Examiner
Art Unit: 3621

Continuation of 11. does NOT place the application in condition for allowance because: As for Applicants' first argument concerning the failure of CyberCash to "identify a network environment and a system policy", the Examiner asserts again that the protocols that CyberCash operates over, TCP/IP, inherently contain these limitations. As for the "network environment and system policy" limitations, consider pages 16-20 of the previously enclosed "RFC 793" - the "Urgent Pointer" is noted as a "means to communicate to the receiver of data that at some point further along in the data stream than the receiver is currently reading there is urgent data. TCP does not attempt to define what the user specifically does upon being notified of pending urgent data, but the general notion is that the receiving process will take action to process the urgent data quickly" (pages 16 and 17, section 2.9, 6). This is both a "network environment" and a "system policy" decision that the sending device has elected to specify.

Additionally, the TCP document cites that the defined options (at the time of inception in 1981) numbered three - "end of option", "no-operation", and "maximum segment size" (section 3.1). The Maximum Segment Size (known as MSS) was well-known to those skilled in the art at the time of the invention as a way of enforcing network policy between two devices that were communicating, as it explicitly defines the "maximum receive segment size at the TCP which sends [the] request". (Examiner notes that while these were the only three options in 1981, there are volumes dedicated to the study of TCP/IP, which cover the more modern systems and encodings - such as TCP/IP Illustrated, Volumes 1-3, by W. Richard Stevens.)

Similarly, TCP/IP contains "flow control" processes in the previously-included RFC 2581 (sections 3.1+). These all allow the TCP subsystem to "select a timing" for providing data, based on the timing of the response that is received from the terminal - see section 3.1: "Slow start ends when…congestion is observed". The Examiner further asserts that the portion of an computer which controls network access (be it the "TCP stack" (software controlling this specific portion of network communication), the "network stack" (software controlling all network communication), the "network card", the "operating system", or even the computer itself) would be the "controller" in the claimed limitation, as all of these portions control some part of network communication.

As for Applicants' arguments concerning claim 10, the Examiner asserts that as "certificate of service" is not explicitly defined in the specification of the instant application, the Examiner may interpret the term as it has been interpreted (see MPEP §904.01). The Examiner notes that all of the messages in CyberCash provide service - furthermore, as many of them are digitally signed (see especially CM6, "pr-signed hash"), the messages are interpreted as "certificates of service".

As for Applicants' arguments that the messages do not contain data concerning the maximum number of times that a certificate can be used, the Examiner asserts that the mere existence of the certificate's data inherently defines the number of times it may be used. As an example, consider an automobile advertisement - the seller of the car would not need to explicitly say that the car's gas tank was refillable, as this is inherent in the definition of automobiles. A "disposable razor" would not need to contain a disclaimer that it is only usable for a number of times before being thrown away. Similarly, the message from client to server which inherently can only be used once would not need a modifier to note that it can only be used once. See MPEP §2112(II) and (IV).

As for Applicants' arguments that management of usage history is unnecessary, Applicants appear to argue that the taking of Official Notice on this is improper, as the certificates used in CyberCash may only be used once. The Examiner notes that "usage history" of certificates was highly well-known to those skilled in the art at the time of the invention, especially in the art of shopping - ideas such as "receipts" have been present for hundreds of years, which give "usage history". More to the point in the present invention, software called "packet loggers" or "packet capture/dump utilities" have been around for many years. These programs capture data, including the data that the CyberCash system uses to communicate. (See especially "Surfing the Tsunami; A large Southeastern university IS team fights off a massive distributed denial of-service attack and lives to tell about it", NetworkWorld, 28 August 2000: section "Noon", "Snort, a packet sniffer/logger…Tcpdump, a packet capture and dump program".) Being that these programs and utilities were well-known to those skilled in the art at the time of the invention, the Examiner feels that the cited portion of MPEP §2144.03 does not apply here.

Finally, Applicants argue that the merchant device in Boesch is not an "authentication and payment device" because it sends the data on to another server for approval. This term, as well, is not explicitly defined by the originally submitted specification. The Examiner notes that the merchant terminal performs "authentication" (as it employs "digital signatures", as cited in the Action) and "payment" (as it communicates with the client device to receive payment information), and therefore is interpreted as an "authentication and payment device" (see MPEP §904.01)..